PANDORA CLOUD
UNPACKING COMPLEXITY

HIPAA & PCI Readiness Checklist

24 controls every regulated SMB should have in place. Plus a 30-day path and a cross-framework view.

A Pandora Cloud Buyer's Resource

May 2026

Pandora Cloud LLC
Women-Owned Small Business (WOSB) | AWS Advanced Partner
GSA MAS: 47QTCA24D00D3 | CAGE: 9JSG7 | UEI: R36GQ3N4XT63
Secret Facility Clearance | pandoracloud.net

About This Checklist

If your business handles Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), processes credit card payments under the Payment Card Industry Data Security Standard (PCI DSS), or both, this checklist tells you in fifteen minutes whether your operation is ready for an audit, a regulator inquiry, or an enterprise security questionnaire.

It is for the small or mid-sized business owners, operations leads, and compliance owners running healthcare practices, healthtech startups, payment-handling SMBs, billing operations, insurance carriers, claims handlers, or any combination of those. The 24 items below are the controls auditors actually test in firms with fewer than 100 people, mapped to specific HIPAA and PCI DSS requirements.

The most useful insight in this checklist is not the score. It is the cross-framework overlap section: most controls that satisfy HIPAA also satisfy PCI DSS, and most that satisfy PCI DSS also satisfy HIPAA. Implement once, document once, and produce framework-specific evidence packages on demand. That is the single biggest cost reduction available to SMBs running both.

Why HIPAA and PCI DSS Matter Now

The compliance pressure on small healthcare and payment-handling businesses has tightened over the past two years.

Office for Civil Rights (OCR) enforcement targets small entities deliberately. OCR has settled multiple HIPAA cases involving practices with fewer than 10 employees in the past 18 months. The Right of Access enforcement initiative specifically targets smaller practices because they are more likely to have unaddressed gaps and OCR uses small-entity settlements to set enforcement examples. "We are too small to audit" is not a viable risk strategy.

Payment Card Industry Security Standards Council moved to PCI DSS v4.0.1 in mid-2024. New requirements for stronger password complexity, expanded multi-factor authentication, more rigorous logging, and continuous monitoring rolled in across 2024 and 2025. Acquiring banks now expect attestations against v4.0.1; older v3.2.1 documents are increasingly rejected.

Cyber insurance underwriting has tightened on both fronts. Underwriters require evidence of HIPAA Security Rule controls and PCI DSS compliance before issuing or renewing policies. Premium deltas between firms with documented compliance and firms without can run 30 to 50 percent.

Enterprise procurement teams ask for both. Healthcare networks, financial institutions, and large insurance carriers running vendor-risk programs increasingly require both HIPAA Business Associate Agreements (BAAs) and PCI DSS attestations from their SMB vendors. Producing both opens contract conversations; missing either ends them.

The 24-item checklist below is the floor. The 30-day roadmap is the path from current state to ready. The cross-framework section is the cost reduction.

What HIPAA and PCI DSS Actually Require

Before scoring yourself, a quick orientation. The two frameworks have different scopes but converge on the same operational controls.

HIPAA Security Rule. Governs the protection of electronic Protected Health Information (ePHI). It applies to "covered entities" (healthcare providers, health plans, clearinghouses) and "business associates" (any vendor that handles PHI on their behalf). The Security Rule has three categories of safeguards (administrative, physical, technical) with about 18 standards and roughly 50 implementation specifications. Penalties for violations are tiered, with annual caps that can reach $2,190,294 per identical provision under the 2025 inflation-adjusted statutory tiers; the Office for Civil Rights also operates an enforcement discretion structure with lower tier-specific caps.

PCI DSS v4.0.1. Governs the protection of cardholder data. It applies to any organization that accepts, transmits, or stores credit card information. The standard has 12 high-level requirements and over 250 sub-requirements; compliance is validated through Self-Assessment Questionnaires (SAQs) or Report on Compliance (RoC) engagements depending on transaction volume and merchant level. Non-compliance fines from card brands typically run $5,000 to $100,000 per month, plus increased transaction fees and potential loss of card-processing privileges.

The overlap is significant. Encryption, access controls, audit logging, vendor management, incident response, and risk analysis controls all map across both frameworks. The control implementation is the same; only the evidence package and framework-specific terminology differ. This is the cost-reduction insight most SMBs miss.

How to Use This Checklist

Walk through the 24 items below with your team. For each item, mark one of:

- Implemented: the control is in place and you have evidence to show it.
- Partial: the control is partially in place; gaps exist.
- Missing: the control does not exist or has not been documented.

Count the implemented items. Use the scoring tiers to determine your readiness state. Then read the cross-framework section to see which controls satisfy both HIPAA and PCI DSS at once; those are your highest-leverage targets.

Section 1: Access and Identity Controls

Access misconfigurations are the most-cited finding category in both HIPAA OCR investigations and PCI DSS Reports on Compliance. Six controls below close the most common gaps.

- [ ] Centralized identity management (Single Sign-On) implemented across all systems handling PHI or cardholder data.
- [ ] Multi-factor authentication enforced for all privileged accounts (HIPAA 164.312(a)(2)(i); PCI DSS Requirement 8.4).
- [ ] Role-based access control with least-privilege permissions for every workforce member.
- [ ] Quarterly access reviews documented with sign-off (HIPAA 164.308(a)(4); PCI DSS Requirement 7.2).
- [ ] Just-in-time access for elevated permissions where the role does not require standing access.
- [ ] Terminated employee access revocation within 24 hours of separation (HIPAA 164.308(a)(3)(ii)(C); PCI DSS Requirement 8.2.5).

Section 2: Data Protection and Encryption

Encryption controls protect data at rest and in transit. Both frameworks require both, with specific cryptographic standards.

- [ ] Encryption at rest enabled for all databases and storage holding PHI or cardholder data using Advanced Encryption Standard (AES) 256-bit or stronger.
- [ ] Encryption in transit (Transport Layer Security 1.2 or higher) enforced for all data flows; weak cipher suites disabled.
- [ ] PHI and cardholder data isolated in dedicated environments not accessible from the public internet (HIPAA 164.312(e)(1); PCI DSS Requirement 1.4).
- [ ] Backup encryption verified across all backup systems and tested through actual restore.
- [ ] Key management policies documented; key rotation schedule defined and operational.
- [ ] Data classification policy in place identifying which systems hold PHI, which hold cardholder data, and which hold both.

Section 3: Monitoring and Evidence

Logs are the backbone of both frameworks. If logs are not collected continuously, retained for the required period, and protected from tampering, the evidence chain breaks.

- [ ] AWS CloudTrail (or Azure Activity Logs / Google Cloud Audit Logs) enabled across all in-scope accounts.
- [ ] AWS Config rules (or equivalent) active for compliance monitoring with automated alerts.
- [ ] Log retention meets regulatory minimums: 6 years for HIPAA per 45 CFR 164.316(b)(2)(i); 1 year minimum for PCI DSS Requirement 10.5.1 with 3 months immediately available.
- [ ] Automated evidence collection in place for control testing artifacts.
- [ ] Incident detection alerts configured for high-risk events (privilege changes, public-access changes, log source going silent).
- [ ] AWS Security Hub or equivalent aggregation active for cross-account findings visibility.

Section 4: Governance and Documentation

The frameworks require documented policies, procedures, and evidence of regular review. Most SMBs have some of these; almost none have all of them in current form.

- [ ] Compliance framework formally documented (which framework applies, which scope, which workforce roles).
- [ ] Risk assessment completed within the last 12 months and updated after any significant system change (HIPAA 164.308(a)(1); PCI DSS Requirement 12.3).
- [ ] Incident response plan documented and tested at least annually with tabletop exercise results.
- [ ] Vendor inventory with compliance verification: every vendor that touches PHI or cardholder data with current Business Associate Agreement (HIPAA) or contractual security obligations (PCI DSS).
- [ ] Business Associate Agreements (BAAs) current for all PHI vendors; expiration tracking active.
- [ ] Change management process documented for production systems with audit trail captured per change.

Cross-Framework Overlap: Implement Once, Satisfy Both

Most regulated SMBs running both HIPAA and PCI DSS implement controls separately for each, write nearly identical policies for each, and burn engineering cycles maintaining redundant evidence packages. The better approach is to map controls cross-framework first, then produce framework-specific evidence views from the same underlying work.

Below are the controls in this checklist that satisfy both HIPAA and PCI DSS simultaneously. If you are running both programs, prioritize these first; they earn double credit per implementation hour.

Control	HIPAA reference	PCI DSS reference
Multi-factor authentication for privileged access	164.312(a)(2)(i)	Requirement 8.4
Encryption at rest (AES-256+)	164.312(a)(2)(iv)	Requirement 3.5.1
Encryption in transit (TLS 1.2+)	164.312(e)(1)	Requirement 4.2.1
Audit logging across in-scope systems	164.312(b)	Requirement 10.2-10.3
Quarterly access reviews	164.308(a)(4)	Requirement 7.2
Vulnerability management	164.308(a)(8)	Requirement 11.3
Incident response plan	164.308(a)(6)	Requirement 12.10
Change management with audit trail	164.312(c)(1)	Requirement 6.5
Annual risk assessment	164.308(a)(1)(ii)(A)	Requirement 12.3
Vendor management with current contracts	164.308(b)(1)	Requirement 12.8
Workforce security awareness training	164.308(a)(5)	Requirement 12.6

That is 11 controls (out of 24 in this checklist) that satisfy both frameworks at once. Map them once, implement them once, and your evidence package builds across both reports. The remaining 13 are framework-specific overlays on top of this shared foundation.

Scoring

Total items implemented (out of 24):

- **20 to 24 items** — Strong posture. Focus on automation, continuous monitoring, and the framework-specific overlays your buyers ask for.
- **12 to 19 items** — Foundations forming, but gaps could expose you during an audit, an OCR investigation, or a PCI assessment. The 30-day roadmap below tells you which gaps to close first.
- **Below 12 items** — Significant gaps. PHI and cardholder data in your environment are at material risk. Start with the Days 1-10 priorities below; the early items are the cheapest to fix and the most consequential.

What to Do With Your Score

The score is only useful if it points to a specific next move.

If you scored 20-24 (Strong): Your foundation is in place. The next investment is the framework-specific overlay your buyers actually ask for. Move toward formal HIPAA risk assessment documentation if you are pursuing OCR audit readiness, or toward PCI DSS Self-Assessment Questionnaire (SAQ) submission if you handle card payments. Consider also pursuing SOC 2 Type II if enterprise buyers are asking for it; the controls you have already implemented satisfy most of SOC 2's Security trust services criterion.

If you scored 12-19 (Foundations Forming): The gaps could surface during an OCR investigation triggered by a complaint or breach, during a PCI quarterly self-assessment, or during a buyer security questionnaire. The fastest path forward is the 30-day roadmap below: pick the section where you have the lowest score and work through the day-by-day plan.

If you scored below 12 (Significant Gaps): You are carrying material regulatory and breach risk. The cost of a HIPAA settlement for an SMB regularly exceeds breach notification, credit monitoring, legal fees, and reputational damage in totals that can reach several million dollars when the full picture is counted. PCI non-compliance fines compound monthly. Start with Days 1-10 of the roadmap; the early items remove the highest-risk exposures.

Your 30-Day HIPAA and PCI Roadmap

This roadmap targets teams scoring Yellow or Red on the 24-item checklist. Strong-foundation teams can compress it; teams with significant gaps may need 60 days.

Days 1 to 10: Identity, access, and the cross-framework wins

Goal: Centralized identity with Multi-Factor Authentication (MFA) enforced. Access reviews scheduled. Departing-employee deprovisioning under 24 hours. The 11 cross-framework controls identified.

- **Day 1-2:** Inventory every system that holds PHI or cardholder data. List the people who have access to each.
- **Day 3-5:** Stand up centralized identity if not already in place. Move every cloud account, Software-as-a-Service (SaaS) app, and internal tool behind it. Enforce MFA for every account.
- **Day 6-7:** Run the access review across all in-scope systems. Document sign-off. Remediate over-privileged accounts.
- **Day 8-9:** Document the deprovisioning procedure with named owner and 24-hour service-level target. Test it with a recent termination if available.
- **Day 10:** Walk through the cross-framework overlap table. Identify which of the 11 dual-purpose controls you have, partial, or missing. The missing ones are your highest-leverage targets.

Days 11 to 20: Encryption, data protection, and vendor management

Goal: Encryption at rest and in transit verified across all PHI and cardholder data stores. Public-access risks remediated. Vendor inventory current with BAAs and contractual obligations verified.

- **Day 11-12:** Audit every storage bucket, database, and file share for encryption-at-rest status using AES-256 or stronger. Turn on encryption for any unencrypted store.
- **Day 13-14:** Verify TLS 1.2 or higher is enforced on every public endpoint and internal service connection handling PHI or cardholder data. Disable weak cipher suites.
- **Day 15-16:** Audit every cloud resource for public-internet exposure. Anything holding regulated data should not be reachable from the public internet without authentication.
- **Day 17-18:** Refresh the vendor inventory. Verify every PHI vendor has a current BAA. Verify every payment-handling vendor has contractual PCI DSS obligations. Triage gaps and assign remediation owners.
- **Day 19-20:** Test backup restore procedures. Pick one critical PHI system and one critical cardholder-data system; attempt full restores; document results.

Days 21 to 30: Logging, monitoring, and program governance

Goal: Continuous logging with retention meeting both framework requirements. At least one automated guardrail active. Risk assessment refreshed. Incident response plan tested.

Day 21-23: Enable cloud-native logging across every account. Centralize the destination. Configure retention to meet both framework minimums (6 years for HIPAA controls all of it; 1 year minimum for PCI DSS with 3 months immediately available).

Day 24-25: Make logs tamper-resistant via immutable storage with versioning. Configure alerts for high-risk events.

Day 26-27: Update the risk assessment. Document identified risks, current mitigations, and accepted residual risks. Capture exceptions in a Plan of Action and Milestones (POA&M).

Day 28-29: Run a tabletop incident response exercise. Document what worked, what did not, and what the plan needs.

Day 30: Re-take the worksheet. Compare scores. The improvement tells you whether the program is working; persistent low-score areas are the next quarter's priorities.

Common Patterns We See

Across SMBs running HIPAA, PCI DSS, or both, the same five gaps show up over and over.

1. The "we have a BAA with our cloud provider" gap. A signed BAA is necessary but not sufficient. It covers the underlying infrastructure; you still own configuration, access, encryption, and audit logging. SMBs that treat the BAA as the compliance ceiling fail audits on the customer-side controls.

2. The "PHI is only in the EHR" assumption. PHI flows through scheduling systems, billing platforms, support ticketing, email attachments, and analytics tools. Your Electronic Health Record (EHR) vendor's compliance covers the EHR; everything else is on you.

3. The cardholder data scope drift. Many SMBs underestimate where cardholder data appears in their environment. Email systems, customer service tools, recorded call audio, and stored receipts all expand PCI DSS scope. The first audit usually surfaces 5-10 systems the team did not realize were in scope.

4. The "annual training is enough" trap. Both frameworks expect periodic, role-relevant security awareness training. Once-a-year click-through training rarely satisfies an auditor; quarterly micro-training plus an annual deep dive is what passes.

5. The "we only worry about it during audit prep" stance. Both frameworks have continuous-operation requirements that point-in-time remediation does not satisfy. Configurations drift, vendors change, employees come and go. Continuous monitoring is the only way to catch drift in real time.

If you scored Yellow or Red, at least three of these patterns are almost certainly the cause.

A Worked Example

A 35-person specialty medical practice handling both PHI and processing patient payments scored 9 of 24 on this checklist. The practice manager believed they were "compliant" because they had signed a BAA with their cloud provider, used an Electronic Health Record system advertised as HIPAA-compliant, and accepted card payments through a major processor.

The 15 missing items included MFA enforcement (only enabled for the senior team), access reviews (never run), encryption verification (assumed but never audited), tamper-resistant logs (logs existed but anyone with admin access could delete them), risk assessment (over 24 months old), and tabletop incident response exercises (never performed).

They worked the 30-day roadmap. By day 10 they had closed seven items. By day 20, four more. By day 30, two more. They scored 22 of 24 on the re-take; the remaining gaps were just-in-time access (deferred to next quarter as a tooling investment) and continuous monitoring of card-handling systems (deferred pending an upgrade to a payment processor that integrated with their identity system).

The cost: roughly 50 hours of practice manager time, 30 hours of contracted security engineer time, and one Saturday for the centralized-identity migration. Total: around $12,000 in external engineering plus internal time. The result: the practice signed a $400,000 multi-year contract with a regional insurance network three months later, which had previously been gated on producing current HIPAA documentation. The 24-item checklist was the diagnostic. The roadmap was the prescription. The contract was the outcome.

Where to Go From Here

The HIPAA and PCI Readiness Checklist sits in a longer compliance journey. Depending on your state and your buyers, the natural next moves:

If you scored Yellow or Red: Start with the 30-day roadmap. Re-score at day 30 to measure progress.

If you handle PHI in cloud-based systems specifically: Pick up the HIPAA Cloud Compliance Checklist. It builds on this one with cloud-specific safeguards. Free at pandoracloud.net/hipaa-cloud-checklist.

If enterprise buyers are asking for SOC 2 Type II: Pick up the SOC 2 Readiness Checklist. The controls you have already implemented for HIPAA and PCI DSS satisfy most of SOC 2's Security trust services criterion. Free at pandoracloud.net/soc2-readiness-checklist.

If you are pursuing federal contracts: Pick up the ATO Readiness Checklist. Free at pandoracloud.net/ato-readiness-checklist.

If you have not yet established the cloud foundation: Take the Cloud Compliance Foundation Worksheet first. It is the entry-point assessment that this checklist builds on. Free at pandoracloud.net/foundation-worksheet.

In every case, the cross-framework controls in this checklist are the highest-leverage investment. Implement once; satisfy multiple frameworks.

Framework Updates to Watch

The compliance landscape is in motion. The citations and controls in this checklist are accurate as of May 2026, but several frameworks have updates in progress that will affect how organizations document and demonstrate compliance over the next 12 to 24 months. If your readiness work is anchored to current rule citations, you are correctly positioned for today; this section names what to watch for.

HIPAA Security Rule (NPRM published January 2025). The Department of Health and Human Services published a Notice of Proposed Rulemaking on January 6, 2025 with substantial proposed changes. The final rule has not yet been issued; it is expected late 2025 or 2026, with a 180-day compliance period after publication. Key proposed changes include: encryption of ePHI at rest and in transit moved from "addressable" to required (with limited exceptions); multi-factor authentication required across relevant systems; removal of the "required vs. addressable" distinction in implementation specifications, making all required with specific exceptions; mandatory vulnerability scanning, asset inventory updates, and tightened risk analysis cadence. This is the most material upcoming change affecting this checklist.

PCI DSS v4.0.1 (current and stable). v4.0.1 became fully mandatory March 31, 2025; v3.2.1 is retired. The next major revision has not been announced; the PCI Security Standards Council typically issues major revisions every 4 to 7 years. Citations in this checklist use v4.0.1 numbering.

SOC 2 / AICPA Trust Services Criteria (stable). The 2017 Trust Services Criteria with revised 2022 Points of Focus remains the current standard. The American Institute of Certified Public Accountants (AICPA) periodically updates Points of Focus without changing the underlying criteria; the framework has been stable for new audits.

NIST 800-53 Rev 5 (stable). Released in 2020 with periodic patches; Patch 6 issued in 2024. NIST has indicated Rev 6 work is in early discussion but no public draft is available; a Rev 6 release is several years out.

FedRAMP (aligned with NIST 800-53 Rev 5). FedRAMP officially moved to Rev 5 in May 2023 with phased Cloud Service Provider transition through 2024 and 2025. FedRAMP follows NIST 800-53 Rev 5 patch updates.

CMMC 2.0 (in phased rollout). The Department of Defense final rule became effective December 16, 2024 with a four-phase rollout: Phase 1 (Level 1 / Level 2 self-assessments) starting November 10, 2025; Phase 2 (Level 2 third-party assessments via C3PAOs) starting November 10, 2026; Phase 3 (Level 3) November 10, 2027; Phase 4 (full implementation) November 10, 2028. If your business sells to defense agencies, Phase 2 is the date most likely to affect your contract eligibility.

NIST 800-171 Rev 3 (published, not yet adopted by CMMC). NIST published 800-171 Rev 3 in May 2024. CMMC Level 2 currently still references Rev 2; the Department of Defense timeline for Rev 3 adoption is unclear but expected in 2026 or 2027. Industry refers to the eventual transition as "CMMC 3.0" though that is not an official term.

What this means for you: HIPAA Security Rule final-rule publication is the most material upcoming change for healthcare and payment-handling SMBs. CMMC Phase 2 (November 2026) is the most material upcoming change for defense-facing SMBs. Everything else is stable for the immediate future.

Printable Scoring Sheet

Print this page. Take it to a conference room. Walk through the 24 items with the team and mark each one. The page is designed to live on a wall or in a binder for the duration of your readiness work.

1. Access and Identity Controls

- ☐ Centralized identity (SSO) across PHI/cardholder systems _____
- ☐ MFA enforced for all privileged accounts _____
- ☐ Role-based access with least privilege _____
- ☐ Quarterly access reviews documented _____
- ☐ Just-in-time access for elevated permissions _____
- ☐ Departing-employee access revoked within 24 hours _____

2. Data Protection and Encryption

- ☐ Encryption at rest (AES-256+) for PHI/cardholder data _____
- ☐ Encryption in transit (TLS 1.2+); weak ciphers disabled _____
- ☐ Regulated data isolated from public internet _____
- ☐ Backup encryption verified through restore test _____
- ☐ Key management policy with rotation schedule _____
- ☐ Data classification policy in place _____

3. Monitoring and Evidence

- ☐ CloudTrail / Activity Logs / Audit Logs enabled _____
- ☐ Config rules active for compliance monitoring _____
- ☐ Log retention: 6yr HIPAA / 1yr PCI (3mo immediate) _____
- ☐ Automated evidence collection in place _____
- ☐ Incident detection alerts for high-risk events _____
- ☐ Security Hub or equivalent aggregation active _____

4. Governance and Documentation

- ☐ Compliance framework formally documented _____
- ☐ Risk assessment within last 12 months _____
- ☐ Incident response plan tested annually _____
- ☐ Vendor inventory with compliance verification _____
- ☐ Current BAAs for all PHI vendors _____
- ☐ Change management process with audit trail _____

Total implemented (out of 24): _____

20-24: Strong posture. Focus on automation and framework-specific overlays.
12-19: Foundations forming; address gaps via the 30-day roadmap.
Below 12: Significant gaps; start with Days 1-10 priorities.

A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business and an Amazon Web Services (AWS) Advanced Tier Partner with a Defense Counterintelligence and Security Agency (DCSA) Secret-level Facility Clearance and Cybersecurity Maturity Model Certification (CMMC) Level 2 self-assessment status. We help regulated SMBs across healthcare, finance, legal, insurance, and defense build compliant cloud environments and operate them as part of normal business, not as periodic audit projects.

If you scored Yellow or Red and want a second set of eyes on which gaps to prioritize, we offer free 30-minute consultations.

Want a second set of eyes on your gaps?

Schedule a free 30-minute consultation. We will walk through your scored checklist and help you prioritize the next 30 days.

pandoracloud.net/#schedule-consultation

Glossary

For readers new to HIPAA and PCI DSS vocabulary, this glossary names the most common terms used in this checklist.

BAA (Business Associate Agreement)
Contract under HIPAA between a covered entity and a third party handling Protected Health Information (PHI). Required for any vendor that touches patient data.

ePHI (Electronic Protected Health Information)
PHI that is created, received, maintained, or transmitted in electronic form. The HIPAA Security Rule applies specifically to ePHI.

EHR (Electronic Health Record)
Digital version of a patient chart. EHR vendors maintain HIPAA-eligible products but configuration responsibility sits with the customer.

MFA (Multi-Factor Authentication)
Login that requires more than just a password. Required for all privileged access under both HIPAA and PCI DSS.

OCR (Office for Civil Rights)
US Department of Health and Human Services agency that enforces HIPAA. Investigates complaints, breach notifications, and tips; imposes civil monetary penalties.

PCI DSS v4.0.1 (Payment Card Industry Data Security Standard)
Industry-mandated standard for organizations handling credit card data. Updated in 2024; replaces v3.2.1.

PHI (Protected Health Information)
Individually identifiable health data covered under HIPAA. Includes 18 specific identifiers ranging from names tied to appointment dates to IP addresses linked to patient portals.

POA&M (Plan of Action and Milestones)
Structured tracking of known compliance gaps with owners, deadlines, and remediation status. Demonstrates that the organization recognizes and manages gaps rather than hides them.

RoC (Report on Compliance)
Detailed PCI DSS compliance report required for higher-volume merchants, prepared by a Qualified Security Assessor (QSA).

SAQ (Self-Assessment Questionnaire)
PCI DSS self-attestation form used by smaller-volume merchants. Various SAQ types apply depending on transaction processing methods.

TLS (Transport Layer Security)
Cryptographic protocol that secures data in transit. Both HIPAA and PCI DSS require TLS 1.2 or higher; weak cipher suites must be disabled.